RACHELE R. BYRD
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com

JON TOSTRUD
TOSTRUD LAW GROUP, PC
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: 310/278-2600
Facsimile: 310/278-2640
jtostrud@tostrudlaw.com

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

THOMAS VICKERY, individually and on behalf of all others similarly situated,

Plaintiff,

-v-

23ANDME, INC.,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff THOMAS VICKERY ("Plaintiff"), on behalf of himself and all others similarly situated, brings this class Action Complaint (the "Action") against Defendant 23andMe, Inc. ("23andMe" or "Defendant"), and alleges the following upon information and belief, except as to allegations concerning Plaintiff himself and his actions, which are alleged upon personal knowledge:

I. INTRODUCTION

1. Plaintiff seeks to hold Defendant responsible for the harm it has caused and will continue to cause to Plaintiff and millions of other similarly situated person as a result of Defendant's inadequate data security policies and practices, which allowed unidentified third parties to download and sell extraordinarily targeted and sensitive personally identifiable information (PII) of Plaintiff and other class members on the Dark Web, including their names, cities and states of residence, genders, years of birth, 23andMe account information, as well as detailed information about Plaintiff and Class Members' genomics, DNA profile, and information about their ancestry and ethnicity (the "Data Breach").

2. While Defendant has publicly stated that the Data Breach was a result of compromised user credentials whereby attackers gained access to data through passwords that users had reused from other websites that were hacked, that explanation is only a fraction of the story. There should have been no way for any unauthorized third parties to be able to download the sensitive PII of any individuals without being detected and stopped. However, Defendant allowed the sensitive PII ***of millions of users*** to be downloaded and offered for sale on a Dark Web hacker forum all without Defendant ever detecting this activity. Indeed, Defendant clearly had no security policies or practices in place to detect or stop this Data Breach from occurring.

3. Companies entrusted with sensitive personal information, such as Defendant who was entrusted with the detailed genetic information of its customers, should do everything possible to protect against cybersecurity incidents, such as the Data Breach. While Defendant clearly did not maintain adequate cybersecurity policies and practices, Defendant marketed itself as operating a privacy and security-centric business. Specifically, Defendant represented on its

main privacy webpage that "we're doing everything in our power to keep your personal data safe."[1]

4. Moreover, Defendant specifically informed prospective customers that "your personally identifiable information (such as your name and email) is stored in in [sic] a separate database from your genetic data so that no one but you (when you use your username and password) can connect the dots between the two" and that, as a result, "even if someone gained access to one of these databases, they could not connect your identity to your genetic data, or vice versa."[2] Defendant also represented to prospective customers that "[w]e meet the highest industry standards for data security. Our information security management system received certification under the globally recognized ISO/IEC 27001:2013, 27018 & 27701 standards after an extensive security audit."[3]

5. Indeed, the Data Breach shows these representations to be false. The hacker(s) here were not only able to access genetic and genomic data for millions of people but, were also able to associate this stolen sensitive PII with the names, years of birth, cities and states of residence, genders, and 23andMe account information of these affected individuals.

6. In addition to violating its specific representations to consumers, Defendant's actions constitute a clear failure to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe and are entitled to injunctive and other equitable relief.

II. PARTIES

7. Plaintiff THOMAS VICKERY is a resident of Virginia and has been a 23andMe customer since July 2023.

[1] *See* 23andMe "Privacy and Data Protection" webpage, https://www.23andme.com/privacy/ (last visited October 29, 2023).
[2] *Id.*
[3] *Id.*

8. Defendant 23andMe, Inc. is Delaware corporation with its principal place of business located at 223 N. Mathilda Avenue, Sunnyvale, California 94086.

III. JURISDICTION AND VENUE

9. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interests and costs, there are more than 100 members of the proposed class, and at least one Class Member is a citizen of a state different from Defendant.

10. This Court has personal jurisdiction over Defendant because Defendant is headquartered and does substantial business from and within in this District.

11. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. STATEMENT OF FACTS

A. Defendant's Business

12. Defendant is a consumer genetics company founded with the mission "to help people access, understand, and benefit from the human genome."[4] Defendant provides consumers with DNA analysis, genetic healthcare information, and genetic ancestry analysis services.

13. In order to use Defendant's services, consumers use a saliva collection kit that Defendant mails to them to collect their saliva at home and mail it back to Defendant's lab in a pre-paid package. Within an average of 3-4 weeks, Defendant analyzes the DNA in the individual's saliva sample and provides detailed personalized reports on everything from the individual's personal genetic health risks and carrier status for various diseases, to the individual's detailed genomics and ancestry profile.[5]

---

[4] https://investors.23andme.com/?_gl=1*ltxxa*_ga*MTcxMDQzMTYwNC4xNjk3MDQ4MDMx*_ ga_G330GF3ZFF*MTY5NzQ5NDM0OS4yLjEuMTY5NzQ5NDM4OC4wLjAuMA (last visited Oct. 29, 2023).

[5] https://www.23andme.com/genetic-science/ (last visited Oct. 29, 2023).

14. The information contained in the individual's genome is then summarized in a report prepared by Defendant, which provides an extraordinarily detailed—and intimate—snapshot of the individual's health risks and disease profile. In addition to detailed information about the individual's health and disease profile, the report prepared by Defendant also contains detailed sensitive information about the individual's ethnic and ancestral background.

15. Defendant also provides pharmacogenetics reports that detail how "[individual'] genetics can influence how [the individuals] process certain medications."[6] Specifically, one type of report Defendant makes available to consumers is called a "Simvastatin Medication Insight report," which provides an analysis of how individuals respond to simvastatin, a commonly-proscribed statin used to lower cholesterol in the blood and reduce the risk of heart attacks, strokes, and heart disease. The report also indicates whether they have an increased chance of experiencing side effects.[7]

B. Defendant's Representations About Security and Privacy

16. Consumers today have dozens of choices for genetic testing services, with some of the leading offerings being AncetryDNA, MyHeritage, Living DNA, FamilyTreeDNA, Nebula Genomics, SelfDecode, and My Toolbox Genomics. In seeking to distinguish itself from the many other genetic testing services available for consumers, Defendant touts its privacy and security practices.

17. For example, Defendant tells consumers, in no uncertain terms on the company's primary "About" webpage, that "[y]ou are in control of your DNA and your data," and that "[w]e believe you should have a safe place to explore and understand your genes. That's why Privacy and Security are woven into everything we do."[8]

18. On Defendant's Privacy and Data Protection webpage, Defendant elaborates on its practices, saying, "When you explore your DNA with 23andMe, you entrust us with important

[6] *See* https://www.23andme.com/topics/pharmacogenetics/slco1b1/?_gl=1*1jvwy6o*_ ga*MTcxMDQzMTYwNC4xNjk3MDQ4MDMx*_ga_G330GF3ZFF*MTY5NzU2MjU0My4zLjEuMTY5NzU2MzU3MC4wLjAuMA (last visited Oct. 29, 2023).

[7] *See* https://blog.23andme.com/articles/new-23andme-report-on-simvastatin (last visited Oct. 29, 2023).

[8] *See* https://www.23andme.com/about/ (last visited Oct. 29, 2023).

personal information. That's why, since day one, protecting your privacy has been our number one priority. We're committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected."[9] Defendant also states, "We meet the highest industry standards for data security. Our information security management system received certification under the globally recognized ISO/IEC 27001:2013, 27018 & 27701 standards after an extensive security audit."[10]

19. In addition to its claims about privacy protections, Defendant claims to understand and prioritize data security and touts its data security practices as a selling point. For example, Defendant represents that "Your data is fiercely protected by security practices that are regularly reviewed and updated. Your genetic information deserves the highest level of security, because without security, you can't have privacy. 23andMe employs software, hardware, and physical security measures to protect your data." Defendant also represents that "while no security standard or system is bulletproof, we're doing everything in our power to keep your personal data safe."[11]

20. Defendant has even claimed to understand the need to stay "a step ahead of hackers," and represented to current and potential customers that it does stay a step ahead of hackers:

> **"What do you do to stay a step ahead of hackers?**
>
> We take multiple steps. First of all, third-party security experts regularly conduct audits and assessments of our systems, ensuring we will never let our guard down.
>
> We encrypt all sensitive information, both when it is stored and when it is being transmitted, so that we make it difficult for potential hackers to gain access."[12]

21. To assure any consumers who may still be concerned about sharing their intimate personal and detailed genetic information with Defendant, Defendant represented that personally identifiable information such as name and email could never be connected with genetic data:

[9] https://www.23andme.com/privacy/ (last visited Oct. 29, 2023).
[10] *Id.*
[11] *Id.*
[12] *Id.*

Anything else you can tell me to put my mind at ease?

> Rest assured that your personally identifiable information (such as your name and email) is stored in in a separate database from your genetic data so that no one but you (when you use your username and password) can connect the dots between the two. That means even if someone gained access to one of these databases, they could not connect your identity to your genetic data, or vice versa."[13]

22. Consumers, including Plaintiff and Class Members, relied on Defendant's representations in choosing Defendant's services and in agreeing to turn over their DNA, and money, to Defendant.

23. Instead of upholding its promises to current and potential customers, Defendant failed to implement and provide adequate data security policies, measures, and procedures to prevent the unauthorized third-party hackers from downloading the PII, including the sensitive PII of millions of users. Indeed, while Defendant assured consumers that "even if someone gained access to [a genetic database] they could not connect your identity to your genetic data, or vice versa,"[14] the Data Breach has showed that representation to false and that Plaintiff's and Class Members' genetic information was easily stolen, sold, and associated with their names and identifying information by the hackers.

C. The Data Breach

24. In an announcement posted to 23andMe's website on October 6, 2023 (the "Announcement"), 23andMe explains:

> "We recently learned that certain 23andMe customer profile information that they opted into sharing through our DNA Relatives feature, was compiled from individual 23andMe.com accounts without the account users' authorization.
>
> After learning of suspicious activity, we immediately began an investigation. While we are continuing to investigate this matter, we believe threat actors were able to access certain accounts in instances where users recycled login credentials – that is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked,
>
> We believe the treat actor may have then, in violation of our Terms of Service, accessed 23andMe.com accounts without authorization and obtained information

[13] *Id.*
[14] *Id.*

> from certain accounts, including information about users' DNA Relatives profiles, to the extent a user opted into that service."[15]

25. Defendant's Announcement failed to provide additional information, including the number of affected individuals or the specific types of information available. However, numerous sources, including some from the Dark Web, show that at least 999,998 individuals were affected by the Data Breach, including Plaintiff and Class Members, that likely more than 7 million users are implicated, and that the hacker clearly targeted individuals of Ashkenazi Jewish decent.

26. On or around October 3, 2023, the hacker responsible for the cyberattack posted on a Dark Web hacker forum claiming to have data for 7 million users—*i.e.*, half of the members of 23andMe—including information about origin estimation, phenotype and health information. To validate the hacker's claim to have this extremely sensitive genetic data, the hacker posted a spreadsheet entitled "Ashkenazi DNA Data of Celebrities" that contained the names and sensitive PII, including genetic information, for 999,998 individuals, and may include the Plaintiff.

27. The PII in the sample spreadsheet posted online includes the name, gender, birth year, profile_id, account_id, location, and ancestral background information of approximately one million individuals of Ashkenazi Jewish decent. It also includes the Y-chromosome haplogroup for all male individuals listed and the mitochondrial DNA haplogroup for all of the listed individuals. These haplogroups provide a specific identification of the ancestral/genetic group that the individuals fall into and can be used to understand not only the specific ancestral lineage(s) the individual belongs in but also likely health-and disease-affecting genetic mutations the individual is likely to possess.

28. In addition to the spreadsheet labeled as containing "Ashkenazi DNA," reports indicate that the 23andMe-derived genetic data of more than 300,000 individuals of Chinese heritage has already been disclosed.[16]

[15] *See* https://blog.23andme.com/articles/addressing-data-security-concerns (last visited October 29, 2023).

[16] *See* https://therecord.media/scraping-incident-genetic-testing-site (last visited Oct. 29, 2023).

D. Defendant Violated Its Obligations to Plaintiff and Class Members

29. The Data Breach exposed Defendant's inadequate cybersecurity and privacy practices as woefully insufficient. While Defendant's announcement states that the information is information the individuals "opted into sharing through [Defendant's] DNA Relatives feature," Plaintiff and Class Members never opted into having this sensitive PII shared with the any unauthorized individuals, and certainly not cybercriminals.

30. More fundamentally, no company entrusted with such intimate personal information, such as Defendant, should have allowed a bad actor to abuse a feature meant to allow people to find and connect with their relatives in order to download the PII of millions of users. Any adequate cybersecurity protocol would have detected the hacker's viewing and exfiltration of a few dozen people's PII and alerted the company and/or cut off access. However, Defendant had no such protections and allowed the actor to exfiltrate the information of more than half of Defendant's customers without being caught.

31. Indeed, the fact that Defendant only announced the Data Breach four days after the hacker posted the stolen PII on a hacking forum suggests that Defendant only "learned" of the Data Breach after the hacker posted, and sold, the information to the Dark Web and not through any security alerts or detectors on Defendant's systems.

32. As a direct result of Defendant's failure to secure and safeguard the sensitive information of customers that entrusted them to do so, all of this sensitive PII is in the hands of cybercriminals. In fact, for the 999,998 Ashkenazi Jewish individuals and roughly 300,000 Chinese individuals, whose sensitive PII was already posted, the PII is now in the hands of cybercriminals and is readily available to download by anyone with access to the hacking forum.

33. At all relevant times, Defendant had a duty to Plaintiff and Class Members by properly securing their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when Defendant became aware that their PII may have been compromised.

34. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the members of the Class relied on Defendant to secure their PII when they entrusted Defendant with the information required to obtain Defendant's services.

35. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in adequate security measures, despite its obligation to protect customers' PII. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

36. Defendant owed a non-delegable duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Private Information against unauthorized access and disclosure.

37. In fact, as detailed above, Defendant's failure to implement and maintain adequate security measures also violated Defendant's representations and promises to its current and prospective customers, on which Plaintiff and Class Members relied in choosing to (i) provide their genetic information to Defendant, (ii) allow Defendant to analyze their DNA to generate summaries of their health and ancestry-related genetics, and (iii) pay Defendant for such services.

38. As a result of the Data Breach, Plaintiff and Class Members suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, lost money paid to Defendant, and the loss of, and diminution in, value of their PII.

39. In addition, Plaintiff's and Class Members' sensitive PII, while compromised and taken by unauthorized third parties, also remains in Defendant's possession. Without additional safeguards and independent review and oversight, it remains vulnerable to future cyberattacks and theft.

40. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect victims' PII.

41. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party.

42. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant and entities like it, and Defendant was thus on notice that failing to take steps necessary to secure the PII against those risks left that property in a dangerous condition and vulnerable to theft. Defendant was further on notice of the severe consequences that would result to Plaintiff and Class Members from its failure to safeguard their PII.

43. Defendant failed to properly monitor the computer network and systems that stored the PII. Instead, had Defendant properly monitored its computer network and systems, it would have discovered the intrusion sooner and could have cut off access to the hacker(s) thereby mitigating the impact of the attack, as opposed to letting cyberthieves roam freely in Defendant's network for and unknown period of time.

44. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

45. Plaintiff and Class Members will incur out of pocket costs for undertaking protective measures to deter and detect identity theft.

46. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

47. Plaintiff seeks remedies including, but not limited to, actual damages, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs. Plaintiff also seeks injunctive and equitable relief to prevent future injury on behalf of himself and the Class.

E. Defendant Failed to Comply with FTC Guidelines

48. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

49. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17]

50. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

51. The FTC further recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

52. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

[17] *See Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016)*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 29, 2023).

[18] *Id.*

53. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect personal, private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

54. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

55. Defendant was at all times fully aware of its obligation to protect the Private Information of its customers, Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

F. Plaintiff Thomas Vickery

56. Plaintiff THOMAS VICKERY is, and at all times relevant, has been a citizen of Virginia. Plaintiff THOMAS VICKERY has no intention of moving to a different state in the immediate future. Plaintiff THOMAS VICKERY received an email to his family from Defendant notifying him that his information was exposed in the Data Breach on October 13, 2023.

57. Plaintiff THOMAS VICKERY provided his PII to Defendant directly in or around August of 2021 in order to obtain ancestry tracing and genomic services from Defendant.

58. Plaintiff THOMAS VICKERY paid Defendant approximately $250 in exchange for these services.

59. Plaintiff THOMAS VICKERY is very careful about sharing his sensitive Private Information. Plaintiff THOMAS VICKERY has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

60. Plaintiff THOMAS VICKERY first learned of the Data Breach in early October online wherein he learned that Defendant had suffered a large data breach. Days later, Plaintiff

THOMAS VICKERY's family received an email directly from Defendant confirming that his PII had been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendant.

61. The Data Breach email indicated that, while the investigation is ongoing, Defendant believes that a threat actor was able to access certain accounts in instances where users employed identical login credentials but does not mention the specific types of PII being affected.

62. While Defendant's investigation is still ongoing, Plaintiff THOMAS VICKERY is concerned he will find the following pieces of his PII listed on a spreadsheet from the hacker forum: name, city and state of residence, gender, 23andMe account information, year of birth, and detailed genetic data.

63. As a result of the Data Breach, Plaintiff THOMAS VICKERY made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification email including but not limited to researching the Data Breach; reviewing bank and financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud; and researching and purchasing additional antivirus, Dark Web monitoring, and credit monitoring services.

64. Plaintiff THOMAS VICKERY has spent more than 20 hours addressing the Data Breach and will continue to spend valuable time for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

65. Plaintiff THOMAS VICKERY suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff THOMAS VICKERY; (b) violation of his privacy rights; (c) the theft of his PII; (d) lost money paid to Defendant and the lost benefit of the bargain in Defendant's failure to comply with its obligations and representations; (e) the out-of-pocket costs of purchasing additional identity theft protection, antivirus, and credit monitoring software; and (f) present, imminent and impending injury arising from the increased risk of identity theft and fraud. In fact, because his

genetic data was impacted, and because his PII was sold and exchanged on the Dark Web, Plaintiff THOMAS VICKERY faces this risk for his lifetime.

66. As a result of the Data Breach, Plaintiff THOMAS VICKERY has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff THOMAS VICKERY is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

67. As a result of the Data Breach, Plaintiff THOMAS VICKERY anticipates spending considerable time and money on an ongoing basis to try to mitigate and/or address any harm caused by the Data Breach. In addition, Plaintiff THOMAS VICKERY will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

V. CLASS ALLEGATIONS

68. Plaintiff brings this action pursuant to the provisions of Rules 23(a),(b)(2), and (b)(3) of the Federal Rules of Civil Procedure ("F.R.C.P.") on behalf of himself and the following classes (collectively, the "Class" or "Class Members" and individually a "Class Member"):

> All individuals in the United States whose PII was exposed to unauthorized third parties as a result of the data breach announced by Defendant on or about October 7, 2023.

69. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel, and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

70. In the alternative, Plaintiff requests additional subclasses as necessary based on the types of PII that were compromised.

71. Plaintiff reserves the right to amend the above Class definitions or to propose other subclasses in subsequent pleadings and motions for class certification.

72. This action has been brought and may properly be maintained as a class action under F.R.C.P. Rule 23 because there is a well-defined community of interest in the litigation and membership of the proposed Classes is readily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Class are so numerous that joinder of all members is impractical, if not impossible. Plaintiff is informed and believes and, on that basis, alleges that the total number of Class Members is at least in the hundreds of thousands of individuals. Membership in the Class will be determined by analysis of Defendant's records and/or through the records made publicly available by the bad actor(s).

b. Commonality: Plaintiff and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

i. Whether Defendant had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using and/or safeguarding their PII;

ii. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

iii. Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

iv. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

v. Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security);

vi. Whether Defendant adequately, promptly and accurately informed Plaintiff and Class Members that their PII had been compromised;

vii. How and when Defendant actually learned of the Data Breach;

viii. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiff and Class Members;

ix. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

x. Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;

xi. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

xii. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Plaintiff in this class action is an adequate representative of the Class in that Plaintiff has the same interest in the litigation of this case as the Class Members, are committed to the vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in their entirety. Plaintiff anticipates no management difficulties in this litigation.

e. Superiority of Class Action: The damages suffered by individual Class Members are significant but may be small relative to each member's enormous expense of

individual litigation. This makes or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately. Individualized litigation increases the delay and expense to all parties and to the court system, presented by the case's complex legal and factual issues. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale and comprehensive supervision by a single court.

73. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, so it is impracticable to bring all Class Members before the Court.

74. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate concerning the Classes in their entireties. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly. Plaintiff's challenge of these policies and practices hinges on Defendant's conduct concerning the Classes in their entirety, not on facts or law applicable only to Plaintiff.

75. Unless a Class-wide injunction is issued, Defendant may continue failing to secure Class Members' PII properly, and Defendant may continue to act unlawfully, as set forth in this Complaint.

76. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under F.R.C.P. Rule 23(b)(2).

VI. CAUSES OF ACTION

COUNT ONE
(Negligence)

77. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

78. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Plaintiff's and Class Members' PII on its computer systems and networks.

79. The duty Defendant owed Plaintiff and Class Members includes but is not limited to (a) the duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession; (b) the duty to protect Plaintiff's and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices and/or its own representations; (c) the duty to implement processes to detect the Data Breach quickly and to act on warnings about data breaches timely; and (d) the duty to promptly notify Plaintiff and Class Members of any data breach, security incident or intrusion that affected or may have affected their PII.

80. Defendant knew or should have known that the PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care to not subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

81. Defendant knew or should have known of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches, including breaches dealing with genetic information of individuals.

82. Defendant knew or should have known that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

83. Because Defendant knew that a breach of its systems could damage numerous individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PII stored thereon.

84. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII that Plaintiff and Class Members had entrusted to it.

85. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PII. This breach of duty includes but is not limited to (a) failing to implement computer systems and data security practices to detect the intrusion and downloading of PII for millions of Defendant's customers; (b) failing to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed; (c) failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Plaintiff's and Class Members' PII, misuse the PII and intentionally disclose it to others without consent; (d) failing to adequately train its employees with respect to security practices that would have prevented or mitigated the extent of the Data Breach; (e) failing to adequately enforce security policies aimed at protecting Plaintiff's and Class Members' PII; and (f) failing to implement processes to quickly detect data breaches, security incidents or intrusions such as the Data Breach in question.

86. As a proximate and foreseeable result of Defendant's negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

87. Further, by explicitly failing to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, and proactive steps to secure their PII.

88. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff's and Class Members' PII and the harm (or risk of imminent harm suffered) by Plaintiff and Class Members. Plaintiff's and Class Members' PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

89. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence. Additionally, Defendant's violation of 15 U.S.C. § 45 constitutes negligence *per se*.

90. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendant maintained belonging to Plaintiff and Class Members; (b) violation of their privacy rights; (c) (iii) the compromise, publication, and/or theft of their PII; (d) lost money paid to Defendant and the lost benefit of the bargain in Defendant's failure to comply with its obligations and representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of the Data Breach; and (f) the present, imminent and impending injury arising from the increased risk of identity theft and fraud.

91. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

92. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its continued possession.

/ / /

/ / /

COUNT TWO
(Breach of Implied Contract)

93. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

94. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

95. Defendant required Plaintiff and Class Members to provide and entrust their PII to it as a condition of obtaining Defendant's services.

96. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

97. As a part of the agreement, as discussed above, Defendant specifically agreed that it would provide security to detect and prevent data breaches and misuse of Plaintiff's and Class Members' PII, to safeguard and protect such non-public information, and to keep such information secure and confidential. Defendant also impliedly agreed to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

98. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII and money to Defendant, in exchange for, amongst other things, the protection of their PII.

99. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

100. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised because of the Data Breach.

101. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendant maintained belonging to Plaintiff and Class Members; (b) violation of their privacy rights; (c) (iii) the

compromise, publication, and/or theft of their PII; (d) lost money paid to Defendant and the lost benefit of the bargain in Defendant's failure to comply with its obligations and representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of the Data Breach; and (f) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

COUNT THREE
(Breach of Implied Covenant of Good Faith and Fair Dealing)

102. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

103. Every contract has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

104. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

105. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members, and continued acceptance of PII and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

106. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT FOUR
(Unjust Enrichment)

107. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

108. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and in so doing provided

Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

109. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

110. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

111. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards and by Defendant's own representations to Plaintiff and Class Members.

112. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

113. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

114. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to Defendant's services.

115. Plaintiff and Class Members have no adequate remedy at law.

116. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendant maintained belonging to Plaintiff and Class Members; (b) violation of their privacy rights; (c) (iii) the compromise, publication, and/or theft of their PII; (d) lost money paid to Defendant and the lost benefit of the bargain in Defendant's failure to comply with its obligations and representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of the

Data Breach; and (f) the present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

117. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendant maintained belonging to Plaintiff and Class Members; (b) violation of their privacy rights; (c) (iii) the compromise, publication, and/or theft of their PII; (d) lost money paid to Defendant and the lost benefit of the bargain in Defendant's failure to comply with its obligations and representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of the Data Breach; and (f) the present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

118. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

119. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT FIVE
(Violation of the California Unfair Competition Law, Cal. Bus & Prof. Code § 17200, *et seq.*)

120. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

121. The California Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200 *et seq*. ("UCL"), prohibits any "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

122. By reason of Defendant's wrongful actions, inaction, and omissions, the resulting Data Breach, as described above, and the unauthorized disclosure of Plaintiff and Class Members' PII, Defendant engaged in unfair practices within the meaning of the UCL.

123. Defendant has violated the UCL by engaging in unfair business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in the UCL with respect to the services provided to the Class.

124. Defendant's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that the PII of Plaintiff and Class Members has been compromised.

125. Defendant's wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and Class Members' PII also constitute "unfair" business acts and practices within the meaning the UCL in that Defendant's conduct was substantially injurious to Plaintiff and Class Members, offensive to public policy, immoral, unethical, oppressive and unscrupulous, and the gravity of Defendant's conduct outweighs any alleged benefits attributable to such conduct.

126. Defendant's business practices as alleged herein are wrongful and unfair because, through the specific statements described above, Defendant is likely to mislead consumers into believing that the PII they provided to Defendant will remain private and secure, when in fact it has not been maintained in a private and secure manner, that Defendant would employ computer systems and practices to prevent the access to and downloading of millions of users' PII, when in fact it did not, and that Defendant would take proper measures to investigate and remediate a data breach such as, when Defendant did not do so.

127. Plaintiff and Class Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendant's unfair competition and violation of the UCL, including but not limited to the price received by Defendant for the services, the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described above.

128. Plaintiff, on behalf of the Class, seeks relief under the UCL, including, but not limited to, restitution to Plaintiff and Class Members of money or property that Defendant may have acquired by means of Defendant's unfair and fraudulent business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unfair business

practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and each member of the proposed Class, respectfully requests that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under Federal Rule of Civil Procedure 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from similar unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

5. For injunctive relief requested by Plaintiff, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to:

   a. An Order requiring Defendant to take appropriate measures to strengthen their data security systems that maintain personally identifying and other information to comply with the applicable state laws according to proof;

   b. An Order requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

6. An order requiring Defendant to pay pre-judgment and post-judgment interest, as provided by law or equity; and

7. Any and all such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury for all issues triable by jury.

Respectfully submitted,

Date: October 31, 2023

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP

By: */s/Rachele R. Byrd*

RACHELE R. BYRD
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com

Date: October 31, 2023

JON TOSTRUD
TOSTRUD LAW GROUP, PC
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: 310/278-2600
Facsimile: 310/278-2640
jtostrud@tostrudlaw.com

Erik H. Langeland
ERIK H. LANGELAND, P.C.
733 Third Avenue, 16th Floor
New York, NY. 10017
Telephone: (212) 354-6270
elangeland@langelandlaw.com

Attorneys for Plaintiff and the Proposed Class

30141v2